STATE OF ALABAMA

Information Technology Standard

Standard 670-05S1: Intrusion Detection/Prevention Systems

1. INTRODUCTION:

Intrusions may be the result of attackers accessing the systems from the Internet, authorized system users who attempt to gain additional privileges for which they are not authorized, and authorized users who misuse the privileges given them. Intrusion detection and prevention systems automate the process of intrusion monitoring and analysis. A properly configured Intrusion Detection System (IDS) can detect unauthorized system access and alert personnel who can contain and recover any resulting damage. An Intrusion Prevention System (IPS) provides another layer of access control, similar to a firewall, and properly configured can deny unauthorized and potentially malicious activity.

2. OBJECTIVE:

Establish the requirements for the deployment of intrusion detection and prevention systems on State of Alabama computer and network resources.

3. SCOPE:

These requirements apply to all State of Alabama networks and application servers.

4. REQUIREMENTS:

> *Policy: State of Alabama organizations shall, in accordance with applicable standards, position intrusion detection and/or prevention capabilities on networks and application servers commensurate with classification and criticality of data processed based on level of risk to unauthorized access.*

Based on the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-31: Intrusion Detection Systems, State of Alabama organizations shall comply with the following requirements pertaining to intrusion detection and prevention systems.

Deploy a combination of network-based and host-based IDS/IPS to protect an enterprise-wide network. Utilize vulnerability analysis products on a regular schedule to test IDS/IPS and other security mechanisms for proper function and configuration.

Utilize Host-based IDS/IPS on application servers that process and store information whose confidentiality, integrity and availability are deemed crucial and where unauthorized access would be detrimental to the State of Alabama.

Utilize Network-Based IDS/IPS on:

- Internet-connected gateways positioned inside the firewall to monitor for unauthorized in-bound traffic
- Demilitarized Zones
- Outside external firewalls
- State of Alabama backbone networks
- Critical subnets

Establish a schedule for checking IDS/IPS log files. The IDS/IPS should be setup to "proactively alert" when a specific condition is recognized. If alerting is setup appropriately, then log file review shall occur weekly. If not setup to alert, then logs shall be monitored daily.

5. DEFINITIONS:

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 670-05: Intrusion Detection/Prevention

6.2 RELATED DOCUMENTS

Signed by Eugene J. Akers, Ph.D., Assistant Director

Revision History

Version	**Release Date**	**Comments**
Original	12/12/2006	